Flipper Zero-Day

Full Documentation | 10-16-2023

Luke Tapanes

Purpose

At the time of writing this, a zero-day exploit has been discovered on the latest version of IOS (17.0.3). There is currently no patch available which is why it is a zero-day vulnerability. The exploit floods an Apple device with packets via Bluetooth and crashes the device, creating a denial-of-service condition. The purpose of this project is to experiment with this exploit myself and understand how this could be used in nefarious ways.

Scope

This is a fairly short and simple project, and the primary goal is to learn about the exploit and how to deliver it with the Flipper Zero. There are a few objectives to complete in order to achieve this goal which are:

- Research the exploit
- Update the Flipper Zero
- Install the firmware with the exploit included.
- Test the exploit.
- Record a video of the exploit in action.

Project

The first step is to research the exploit to get a better understanding of what is going on in the back end and also how to obtain and use the exploit for myself. To do this, I went to my favorite platform, YouTube, and watched a few videos which can be visited by the links below.

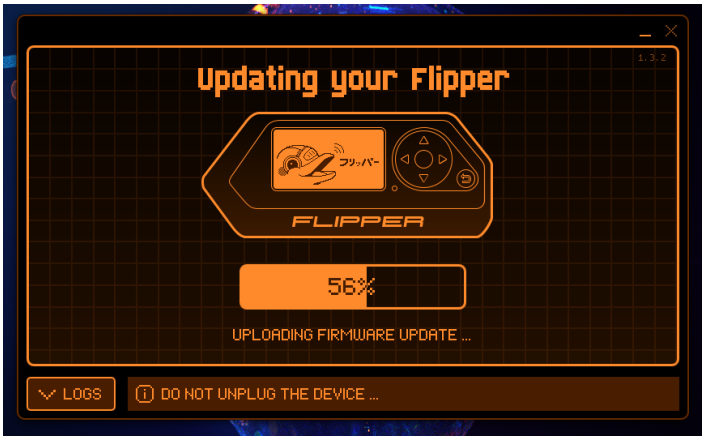
https://www.youtube.com/watch?v=d8cSKNmBwX4&pp=ygUMZmxpcHBlciB6ZXJv

https://www.youtube.com/watch?v=pD8jze5fCHA&pp=ygUMZmxpcHBlciB6ZXJv

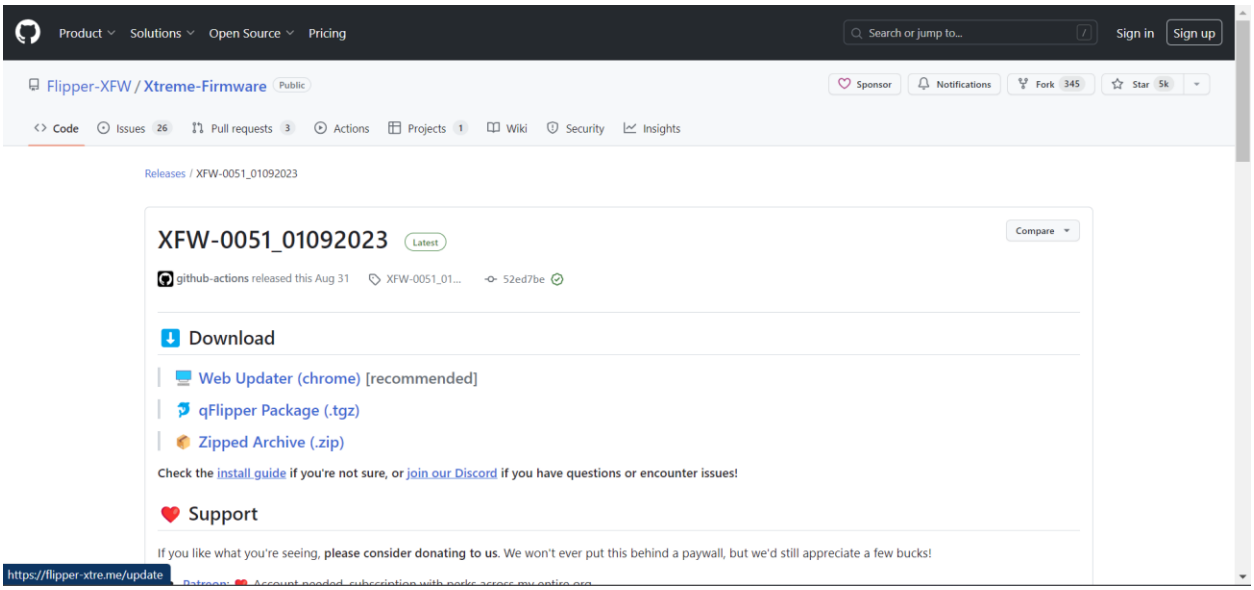
https://www.youtube.com/watch?v=MJd6qugqHg8&t=562s&pp=ygUMZmxpcHBlciB6ZXJv

After gaining a better understanding of the project, it is time to perform it myself. First, I navigate to Flipper's main website and download the application needed to update the firmware on the flipper. This can be seen in the screenshot below.

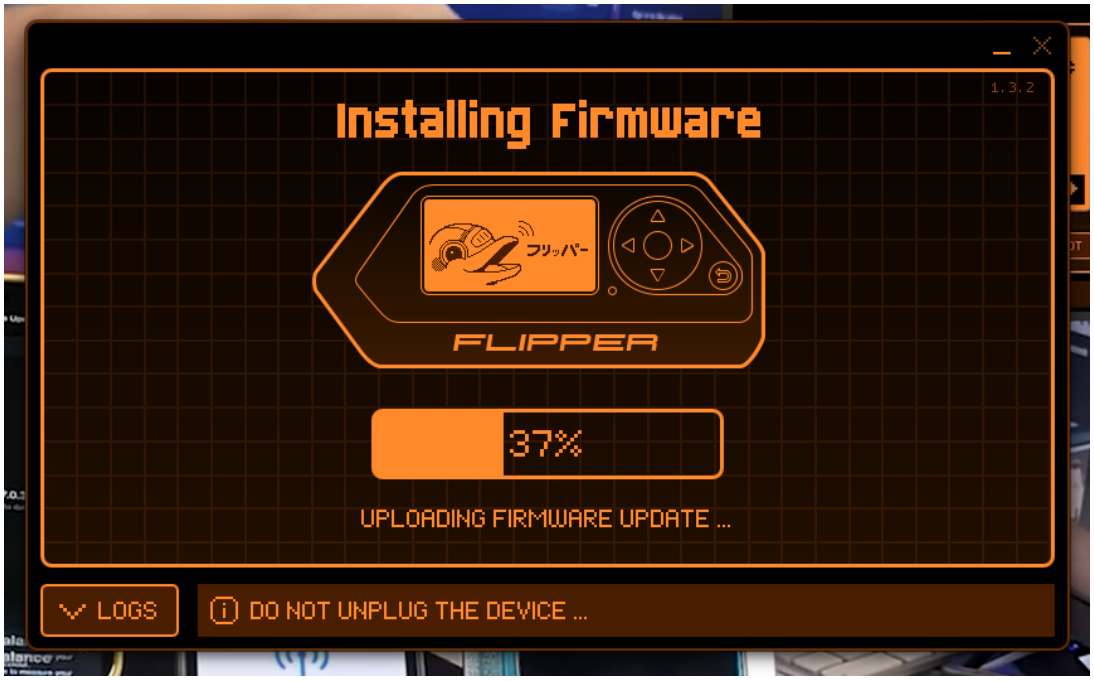
After downloading the application, I connected my Flipper Zero to my computer and updated its firmware.



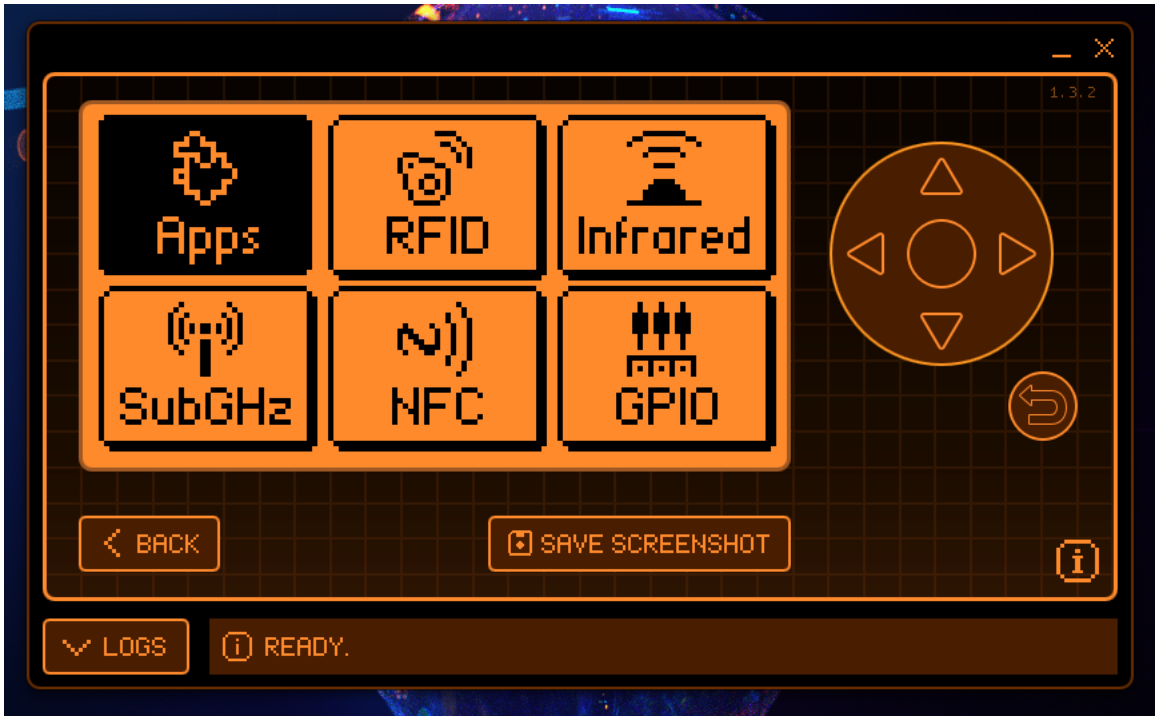
Updating the firmware is technically unnecessary since I need to install new firmware anyways. I updated the current firmware to avoid any issues just in case. Now that the firmware is updated, I navigated to GitHub where the custom firmware was located. This custom firmware is what contains the exploit and a few other tools developed by the community.

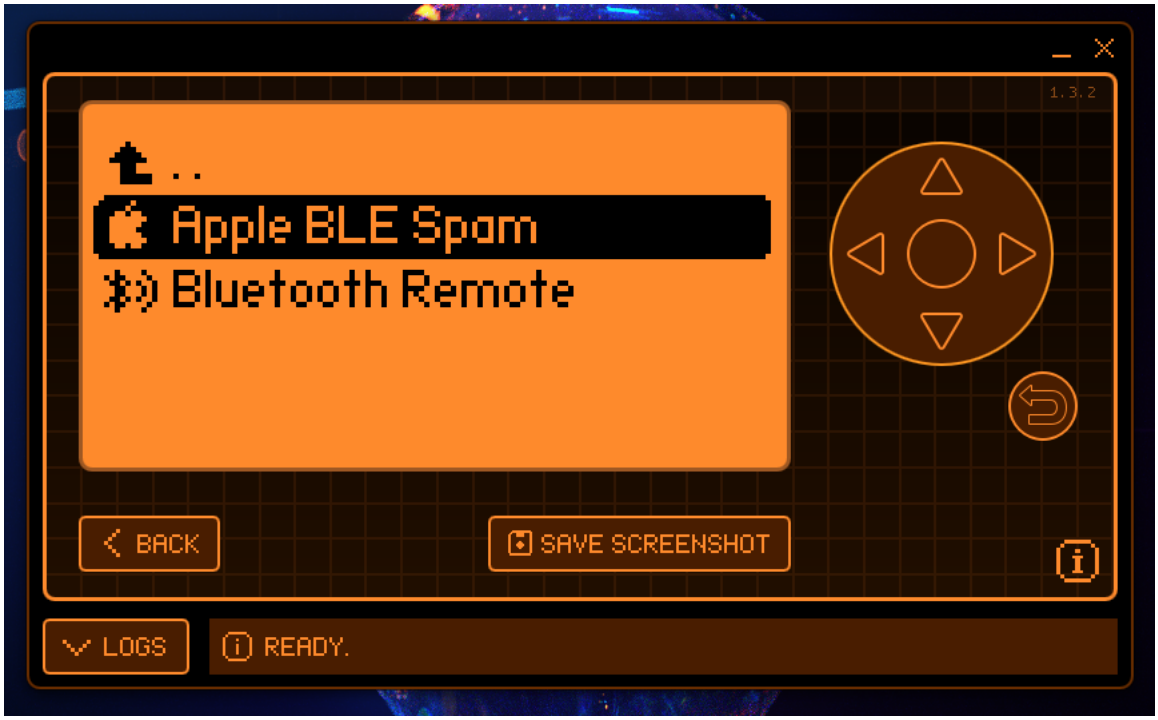


Now that the firmware is downloaded, it is time to install it on the Flipper Zero. This process is similar to updating the firmware as seen previously. This can be seen in the screenshot below.

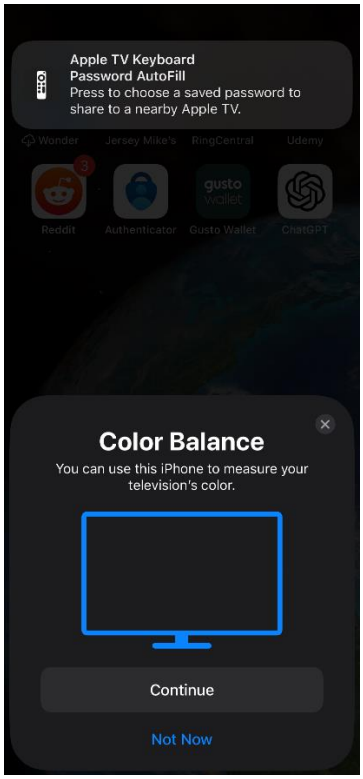


Now that the new firmware has successfully been installed, I verified that the exploit is on the device. To do this, I navigated the interface and clicked on “Apps” then “Bluetooth.” Sure enough, the exploit was there which is labeled “Apple BLE Spam.” This can bee seen in the screenshots below.





Now that I successfully obtained the exploit on my Flipper Zero, it is time to test it. To do this, I used my phone. I recorded a video of the exploit in action which can be viewed here. The screenshot below is an example of the messages that get flooded on the phone prior to the crash.



Lessons Learned

This was a fascinating project to complete as it was the first zero-day vulnerability that I have experimented with. It is a crazy feeling to be able to pull off this exploit and not have an available patch to defend against it. There are only two ways to prevent this attack from occurring. One of which is by disabling Bluetooth in the settings. The other is by being out of the vicinity of the Bluetooth range. As mentioned in the beginning of this write up, this attack creates a denial-of-service condition, which can be used for many nefarious purposes. One example would be to prevent someone from making a phone call, which could be a very important call.